Pearson BTEC Level 3 Nationals Diploma, Extended Diploma

Window for supervised period:
Tuesday 10 January 2023 – Monday 30 January 2023

Supervised hours 5 hours

Paper reference **20158K**

Information Technology

UNIT 11: Cyber Security and Incident Management

Part A

You must have:
Risk_Assessment.rtf
Security_Plan.rtf

Instruction

- **Part A** and **Part B** contain material for the completion of the set tasks under
- supervised conditions.
- There are 43 marks for **Part A** and 37 marks for **Part B**, giving a total mark for the set tasks of 80.
- **Part A** and **Part B** are specific to each series and this material must be issued only to learners who have been entered to take the tasks in the specified series.
- Learners must only have access to **Part A** during this supervised assessment period.
- This booklet should be kept securely until the start of the 5-hour, **Part A** supervised assessment period.
- **Part A** will need to have been completed and kept securely before starting **Part B**.
- **Part B** materials must not be accessed during completion of **Part A**.
- Both parts will need to be completed during the 3-week period timetabled by Pearson.
- **Part A** and **Part B** tasks must be submitted together for each learner.
- This booklet should not be returned to Pearson.
- Answer **all** activities.

Information

- The total mark for this Part is 43.

Turn over ▶

Pearson

Instructions to Invigilators

This paper must be read in conjunction with the unit information in the specification and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document. See the Pearson website for details.

Refer carefully to the instructions in this task booklet and the *BTEC Nationals Instructions for Conducting External Assessments (ICEA)* document to ensure that the assessment is supervised correctly.

Part A and **Part B** set tasks should be completed during the period of 3 weeks timetabled by Pearson. **Part A** must be completed before starting **Part B**.

The 5-hour **Part A** set task must be carried out under supervised conditions.

The set task can be undertaken in more than one supervised session.

Electronic templates for activities 1 and 2 are available on the website for centres to download for learner use.

Learners must complete this task on a computer using the templates provided and appropriate software. All work must be saved as PDF documents for submission.

Invigilators may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

Invigilators should note that they are responsible for maintaining security and for reporting issues to Pearson.

Maintaining Security

- Learners must not bring anything into the supervised environment or take anything out.
- Centres are responsible for putting in place appropriate checks to ensure that only permitted material is introduced into the supervised environment.
- Internet access is not permitted.
- Learner's work must be regularly backed up. Learners should save their work to their folder using the naming instructions indicated in each activity.
- During any permitted break, and at the end of the session, materials must be kept securely and no items removed from the supervised environment.
- Learners can only access their work under supervision.
- User areas must only be accessible to the individual learners and to named members of staff.
- Any materials being used by learners must be collected in at the end of each session, stored securely and handed back at the beginning of the next session.
- Following completion of **Part A** of the set task, all materials must be retained securely for submission to Pearson.
- **Part A** materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

Each learner must create a folder to submit their work. Each folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

Each learner will need to submit 3 PDF documents within their folder.

The 3 PDF documents should use these file names:

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

An authentication sheet must be completed by each learner and submitted with the final outcomes.

The work should be submitted no later than 1 February 2023.

Instructions for Learners

Read the set task information carefully.

Plan your time carefully to allow for the preparation and completion of all the activities.

Your centre will advise you of the timing for the supervised period. It is likely that you will be given more than one timetabled session to complete these tasks.

Internet access is not allowed.

You will complete this set task under supervision and your work will be kept securely at all times.

You must work independently throughout the supervised assessment period and must not share your work with other learners.

Your invigilator may clarify the wording that appears in this task but cannot provide any guidance in completion of the task.

You should only consider threats, vulnerabilities, risks and security protection measures that are implied and/or specified in the set task brief.

Part A materials must not be accessed during the completion of **Part B**.

Outcomes for Submission

You must create a folder to submit your work. The folder should be named according to this naming convention:

[Centre #]_[Registration number #]_[surname]_[first letter of first name]_U11A

Example: Joshua Smith with registration number F180542 at centre 12345 would have a folder titled

12345_F180542_Smith_J_U11A

You will need to submit 3 PDF documents within this folder.

The 3 PDF documents should use these file names:

Activity 1: activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]

Activity 2: activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]

Activity 3: activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]

You must complete an authentication sheet before you hand your work in to your invigilator.

Set Task Brief

Guiding Lighting

Paul Jones is the owner of Guiding Lighting (GL). The business makes and maintains lighting systems for emergency routes such as fire exits. The lighting systems include illuminated information panels and lights built into floors and walls to indicate the route that people should use to find the nearest exit in an emergency.

GL has its headquarters at a location near Swindon. **Figure 1** is a plan of the site.

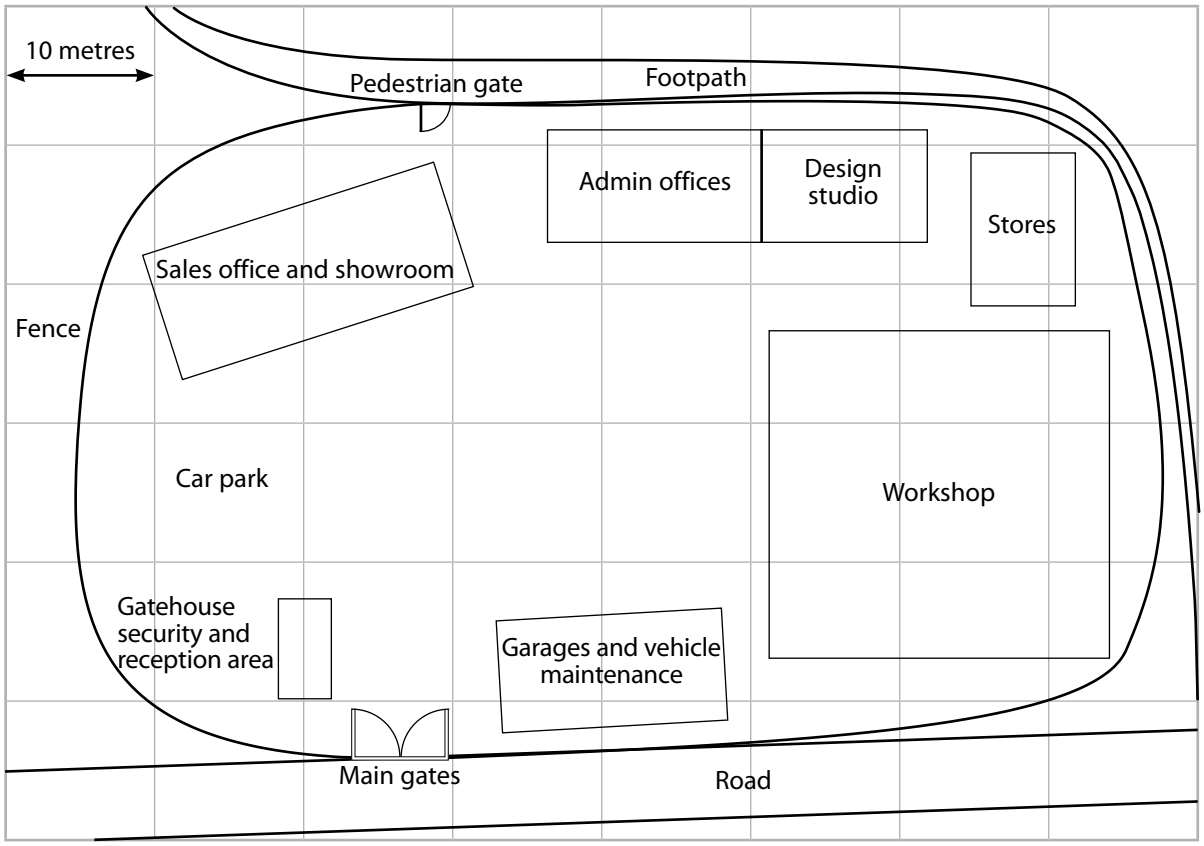

Figure 1

GL also has nine regional offices that cover most of England and Wales. These offices have sales and technical staff who handle installation and maintenance of the lighting systems. All product development and manufacturing takes place at the Swindon location.

GL has developed its lighting systems to include smart lighting that is part of the Internet of Things (IoT). These lights can link to networks and can respond to the input from sensors. Paul is developing a new product that makes use of IoT technology.

Paul has seen town centres in Spain where coloured lines are painted onto the streets. Tourists can obtain a booklet or audio guide from a Tourist Information Office and then follow the lines to visit landmarks, museums and other tourist attractions. Paul is developing a system where GL's smart lighting in an IoT network replaces the painted lines.

The devices in the IoT network will connect to each other using the Zigbee protocol. Zigbee is a low-power WiFi protocol that incorporates mesh networking and uses IPv6 addresses.

Tourists will download an app onto a mobile device and select the places that they wish to visit. The app then calculates the best route and the smart lighting will guide the tourist from place to place. The app will connect to the IoT network using WiFi or Bluetooth.

Paul has many years of management experience and regards himself as a competent IT user. He has written the app and created a working prototype that guides visitors around GL's headquarters. This is shown in **Figure 2**.

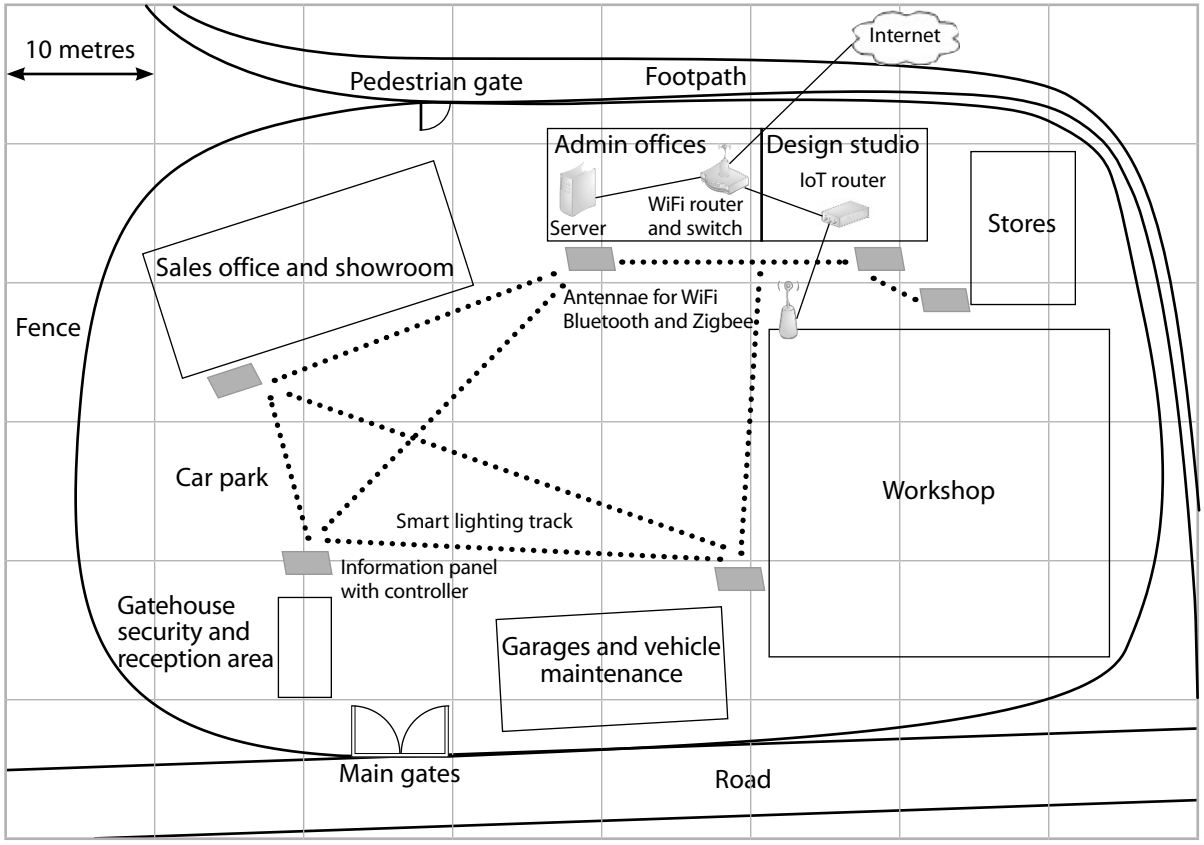

Figure 2

GL's current systems for emergency routes are located inside buildings and can only be controlled by wired components such as alarm buttons or smoke detectors. Paul is aware that his tourist guide system will be much more accessible to the public and will need to have wireless connectivity.

Paul thinks it would be a good idea to have someone who is not employed by the company to advise on the system before one is deployed for use with the public. He has hired you to advise on cyber security and incident management.

Development plan

At a meeting with Paul you establish that:

1. Network connectivity for future systems must conform to that of the prototype, **Figure 2**.
2. The network must be easily scalable.
3. WiFi and Bluetooth connectivity should be available for a wide range of mobile devices.
4. IoT devices include the IoT router, the information panels and controllers, the lighting tracks, and the antennae.
5. Other IoT devices may be added to future deployments of the system.
6. The IoT router must be the only point of connection between the IoT network and any other network.
7. Administrative access to the IoT network must only be available via the IoT router in order to prevent an attack via the internet.
8. For administration and maintenance purposes, GL must be able to connect to any installed system from its offices, via the internet.
9. The app must be able to interact with the IoT devices/network but not be able to make changes to any settings as it may be misused to attack a system.
10. Paul requires high availability and reliability from the system.
11. Public/guest interfaces to the system must be available in many different languages.

Part A Set Task

You must complete ALL activities in the set task.

Read the set task brief carefully before you begin and note that reading time is included in the overall assessment time.

Paul has hired you to advise on cyber security and incident management.

You should only consider threats, vulnerabilities, risks and protection measures that are implied and/or specified in the set task brief.

Design cyber security protection measures for the given prototype computer network.

Activity 1: Risk assessment of the networked system

Duplicate (copy and paste) and complete the risk assessment using the template given for each threat.

Produce a cyber security risk assessment using the template **Risk_Assessment.rtf**

Save your completed risk assessment as a PDF in your folder for submission as **activity1_riskassessment_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour and 30 minutes on this activity.

(Total for Activity 1 = 8 marks)

Activity 2: Cyber security plan for the networked system

Using the template **Security_Plan.rtf** produce a cyber security plan for the computer network using the results of the risk assessment.

For each protection measure, you must consider:

(a) threat(s) addressed by the protection measure
(b) action(s) to be taken
(c) reasons for the action(s)
(d) overview of constraints – technical and financial
(e) overview of legal responsibilities
(f) overview of usability of the system
(g) outline cost-benefit
(h) test plan.

Duplicate (copy and paste) and complete the cyber security plan using the template given for each protection measure, as appropriate.

Save your completed security plan as a PDF in your folder for submission as **activity2_securityplan_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 2 hours and 30 minutes on this activity.

(Total for Activity 2 = 20 marks)

Activity 3: Management report justifying the solution

Produce a management report, justifying how the proposed cyber security plan will meet the security requirements of the set task brief.

The report should include:

- an assessment of the appropriateness of your protection measures
- a consideration of alternative protection measures that could be used
- a rationale for choosing your protection measures over the alternatives.

Save your completed management report as a PDF in your folder for submission as **activity3_managementreport_[Registration number #]_[surname]_[first letter of first name]**

You are advised to spend 1 hour on this activity.

(Total for Activity 3 = 12 marks)

TOTAL FOR TECHNICAL LANGUAGE IN PART A = 3 MARKS
TOTAL FOR PART A = 43 MARKS